AMENDMENT TO THE CLAIMS

Please add new claim 21 as follows:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Previously Presented) A hardware implementation of a crypto-function comprising:

a first register storing data to be encrypted or decrypted;

a second register for receiving data which has been encrypted or decrypted; and

combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle,

wherein the combinational logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory.

2. (Original) The hardware implementation of a crypto-function recited in claim 1, wherein the crypto-function is a block cipher algorithm.

3. (Original) The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the Data Encryption Standard (DES) algorithm.

4. (Original) The hardware implementation of a crypto-function recited in claim 2, wherein the crypto-function is the CHAIN algorithm.

5. (Original) The hardware implementation of a crypto-function recited in claim 2, wherein the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times.

6. (Previously Presented) The hardware implementation of a crypto-function recited in claim 5, wherein the combinational logic performs mixing, permutation and key-dependent substitution in each round.

7. (Original) The hardware implementation of a crypto-function recited in claim 5, wherein the combinational logic enciphers a block by performing an initial permutation of a block to be enciphered and then a complex key-dependent computation followed by a permutation which is an inverse of the initial permutation.

8. (Original) The hardware implementation of a crypto-function recited in claim 7, wherein the combinational logic deciphers a block by performing deciphering using the same key as used to encipher the block in a process that is an inverse of the enciphering process.

9. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the one hardware cycle is approximately ten clock cycles.

10. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the hardware implementation of the crypto-function uses only the combinational logic without having to store intermediate results in registers.

11. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the hardware implementation of the crypto-function computes an iterated round function in one clock cycle.

12. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the combinational logic utilizes a Data Encryption Standard (DES) algorithm that is implemented in the combinational logic.

13. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the crypto-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read.

14. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the combinational logic utilizes logic circuits without memory,

whereby no registers are used to store intermediate results or iterations of enciphering or deciphering computations.

15. (Previously Presented) The hardware implementation of a crypto-function recited in claim 1, wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read.

16. (Previously Presented) A hardware implementation of a crypto-function comprising:

a first register that stores data to be encrypted or decrypted;

a second register that receives data which has been encrypted or decrypted; and

combinational logic that performs computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle, the combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory,

wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read.

17. (Previously Presented) The hardware implementation of a crypto-function recited in claim 16, wherein the single hardware cycle is approximately ten clock cycles.

18. (Previously Presented) The hardware implementation of a crypto-function recited in claim 16, wherein the hardware implementation of the crypto-function computes an iterated round function in just one clock cycle.

19. (Previously Presented) A hardware implementation of a crypto-function comprising:

a first register that stores data to be encrypted or decrypted;

a second register that receives data which has been encrypted or decrypted; and

combinational logic that performs computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle, the combinational logic comprising logic functions whose outputs depend solely on their inputs and utilizing logic circuits without memory,

wherein the single hardware cycle comprises several clock cycles.

20. (Previously Presented) The hardware implementation of a crypto-function recited in claim 19, wherein the crypt-function is implemented in the combinational logic without intermediate registers that require loading and settling time before contents of the intermediate registers can be read.

21. (New) A hardware implementation of a crypto-function comprising:

a first register storing data to be encrypted or decrypted, wherein inputs to the first register are bits from an initial value accumulator, a data register, and a key register;

combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to a second register in a single hardware cycle;

bits from the initial value accumulator and the data register are exclusive ORed and then subjected to an initial permutation in a permutation logic;

an output of the permutation logic comprising a logic block performing a key-dependent computation which involves a key schedule; and

an output of the key register being subjected to a permutation choice in another permutation logic,

wherein the combinational logic comprises logic functions whose outputs depend solely on their inputs and utilizes logic circuits without memory.